



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



**065.021 Kentucky Online Gateway (KOG)
Application Configuration Management Policy**


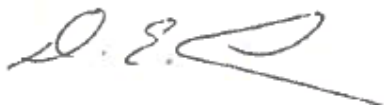
**Version 1.0
October 5, 2018**

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

Revision History

Date	Version	Description	Author
10/5/2018	1.0	Effective Date	CHFS OATS Policy Charter Team
10/5/2018	1.0	Review Date	CHFS OATS Policy Charter Team
10/5/2018	1.0	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/5/2018	Jennifer Harp	
CHFS Chief Information Security Officer (or designee)	10/5/2018	DENNIS E. LEBER	

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	ROLES AND RESPONSIBILITIES	7
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	7
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	8
4.1	GENERAL	8
5	POLICY MAINTENANCE RESPONSIBILITY	9
6	POLICY EXCEPTIONS	9
7	POLICY REVIEW CYCLE.....	9
8	POLICY REFERENCES	10

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

1 Policy Definitions

- **Access:** The ability to use or modify an information resource.
- **Application:** A software program designed to perform a specific function (e.g., Partner Portal, Benefind, etc.).
- **Business Partner:** The agency in which the system/data owner has granted permission for use of a designated application.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

- **System/Data Administrator:** An individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services this role is generally played by a CHFS Branch Manager.
- **System/Data Custodian:** An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky this role is generally played by Commonwealth Office of Technology (COT).
- **System/Data Owner:** The person who has final agency responsibility of data protection and is the person held liable for any negligence when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data, usually a senior executive, designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services this role is generally played by a CHFS Business Executive.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.
- **Worker Type:** Logical containers in which workers are grouped, based on the application access required and the type of work that they perform in order to fulfill their job responsibilities.

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through configuration management guidelines. This document establishes the agency's Application Configuration Management Policy, which helps manage risks and provides guidelines for privacy and security best practices regarding the configuration of applications housed in the Kentucky Online Gateway (KOG).

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Advisor have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible to adhere to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in [section 8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) will be responsible to work with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

4 Policy Requirements

4.1 General

The purpose of this policy is to ensure all application configuration requests and updates are reviewed and implemented in a rational and predictable manner. Effective application and enforcement of these standards is essential to ensuring reliable delivery of services.

Application Owners are responsible for the following when requesting new application configurations, role configurations, URL configurations and/or changes to current configurations within KOG:

1. A completed Request for Configuration Form shall be submitted via email to the KOGApplicationConfiguration@ky.gov inbox at least forty-eight (48) hours prior to requested deployment date. The following information is to be included on the Request for Configuration form:
 - a. Application Configuration Information
 - b. Application Role Details
2. Business partners responsible for submitting provisioning access request for users
3. Approval workflow and/or credential workflow process for access request, including named workflow approvers
4. Requirement for initial access for users, either through bulk load or individual access request by designated business partners

Once the new application configuration has been completed by the KOG Technical Team, training will be provided by the KOG Business Team to the Application Owner(s) if required. The configuration will then be assigned to the KOG Technical Team for configuration of the Relying Party Trust in Active Directory Federation Services (ADFS) and the provisioning of user accounts. Upon completion of the application configuration by the KOG Technical Team, a notification will be sent to the Application Owner for provisioning staff.

Once the initial provisioning has been completed, additional access requests to the application must be granted as follows:

- If provisioning was completed through a bulk load, any additional users must be added through the Access Request process initiated by the Business Partners, which can be found in the KOG Request Application.
- Provisioning of additional worker types will be granted through the Application Owner via email to the KOGWorkerTypeChanges@ky.gov.

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

When Application access is granted by submitting an Access Request through KOG, the action goes through an approval workflow process before the Application can be accessed by the end user through KOG. The approval workflow contains named individuals responsible for approving employee access within the organizational structure, therefore it is the responsibility of the Application Owner and/or designated Business Partner's to notify the KOG team of staffing changes resulting in additions and deletions to the workflow. Failure to notify the KOG team of these staffing changes can result in a delay and/or denial of workflow request submitted through the KOG request application. Updates to the workflow can be submitted via email to the KOGHelpdesk@ky.gov. All email request will be retained for a period of five (5) years from the date of the request.

When an application, or role within an application, is no longer utilized, the Application Owner will be required to send the request to remove the application or role from the existing worker type templates. This request is to be submitted via email to the KOGHelpdesk@ky.gov. All request submitted to KOG will be completed within forty-eight (48) business hours.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in [CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#).

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who are not on boarded or utilizing KOG, the [COT F181EZ Form](#) shall be used to request any action (create, modify, or delete) related to CHFS domain accounts/access. Once forms are completed and approved, they must be submitted to CHFSServiceRequests@ky.gov for completion. Please refer to the [COT Forms Page](#) for instructions and more detailed information.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

065.021 KOG Application Configuration Management Policy	Current Version: 1.0
065.000 Application Development	Review Date: 10/05/2018

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Form: Request for Configuration Form
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Form Instructions: F181EZ- Staff Service Request, EZ Version, Form Instructions
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Online Gateway (KOG)
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information